AMA1007 Supplementary Notes: Hill Cipher

Consider the following mapping from characters (including some special characters) to numbers from 0 to 28:

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9

K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z	.	?	_
20	21	22	23	24	25	26	27	28

Consider a message we would like to encrypt: "LINEAR_ALGEBRA?".

According to the above assignment of characters to numbers, the message can be converted to:
"11, 8, 13, 4, 0, 17, 28, 0, 11, 6, 4, 1, 17, 0, 27 ".

Then, we get any invertible 3×3 matrix, say, $\boldsymbol{A} = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$. This invertible matrix is called the Hill-3-cipher matrix. We can use this to convert the message 3 characters at a time.

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 11 \\ 8 \\ 13 \end{bmatrix} = \begin{bmatrix} 66 \\ 21 \\ 19 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 4 \\ 0 \\ 17 \end{bmatrix} = \begin{bmatrix} 55 \\ 17 \\ 4 \end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 1\\1 & 1 & 0\end{bmatrix}\begin{bmatrix}28\\0\\11\end{bmatrix} = \begin{bmatrix}61\\11\\28\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 1\\1 & 1 & 0\end{bmatrix}\begin{bmatrix}6\\4\\1\end{bmatrix} = \begin{bmatrix}17\\5\\10\end{bmatrix}$$

$$\begin{bmatrix}1 & 2 & 3\\0 & 1 & 1\\1 & 1 & 0\end{bmatrix}\begin{bmatrix}17\\0\\27\end{bmatrix} = \begin{bmatrix}98\\27\\17\end{bmatrix}$$

Thus, the above message is now:
"66, 21, 19, 55, 17, 4, 61, 11, 28, 17, 5, 10, 98, 27, 17 ".

Then, we take the values modulo 29 (that is to say, when the number exceeds 28, we divide it by 29 and get the remainder; that is the same as, to add or subtract integer multiple of 29 to the number to make it within the range from 0 to 28.). Thus, the encrypted message is:
"8, 21, 19, 26, 17, 4, 3, 11, 28, 17, 5, 10, 11, 27, 17 ".
Mapping the numbers back to characters, we have: "IVT. REDL_RFKL?R".

The message is then transmitted to the other party.

To recover the original message, the receiver would need to multiply the message with $\boldsymbol{A}^{-1} = \begin{bmatrix}1/2 & -3/2 & 1/2\\-1/2 & 3/2 & 1/2\\1/2 & -1/2 & -1/2\end{bmatrix}$. For example, the first three characters, multiply with $\boldsymbol{A}^{-1}$:

$$\begin{bmatrix}1/2 & -3/2 & 1/2\\-1/2 & 3/2 & 1/2\\1/2 & -1/2 & -1/2\end{bmatrix}\begin{bmatrix}8\\21\\19\end{bmatrix} = \begin{bmatrix}-18\\37\\-16\end{bmatrix}.$$

Since the result is out of the range from 0 to 28, we apply Modular arithmetic again (that is to say, add or subtract integer multiple of 29 to the number to make it inside the range from 0 to 28). Thus

$$\begin{aligned}-18+29 &= 11\\37-29 &= 8\\-16+29 &= 13.\end{aligned}$$

Thus, we recover the first three characters "LIN".